


# SSL Benchmarks

• • •



*SSL performance testing comparison  
of Intel<sup>®</sup> Itanium<sup>™</sup> architecture and  
Sun<sup>®</sup> UltraSPARC-II<sup>™</sup> architecture*

*Anthony Saadeh  
Coradiant Inc.  
April 2001*

# SSL Benchmarks

## *SSL performance testing comparison of Intel<sup>®</sup> Itanium<sup>™</sup> architecture and Sun<sup>®</sup> UltraSPARC-II<sup>™</sup> architecture*

### **Abstract**

Coradiant Research, formerly known as Networkshop, is an authority on SSL performance benchmarking. Coradiant Research is the research arm of the premier managed service provider Coradiant Inc (<http://www.coradiant.com/>).

Critical issues for today's e-business are Web server SSL connection capacity and latency. As a data transport medium, the Internet can be unreliable. Network conditions, such as overburdened networks, telecommunication company peering points with packet loss, etc, play a major factor in the end-user's perceived experience and satisfaction. Network related problems coupled with overburdened servers (servers that cannot process connections and requests within the end-user "patience time limit<sup>1</sup>"), further amplify this challenge and will result in e-business loss for corporations. As more organizations turn to SSL processing, even for non-confidential data, processing secure connections and delivering content quickly, will play a major factor in organizations' Internet e-business presence.

Coradiant Research benchmarked the SSL connection capacity and latency of the Intel<sup>®</sup> Itanium<sup>™</sup> (Itanium<sup>™</sup>) processor. We also compared the architectures of the Itanium<sup>™</sup> processor to the Sun<sup>®</sup> UltraSPARC-II processor.

Coradiant Research benchmarked the following servers: Itanium<sup>™</sup> processor based server; and the Sun Enterprise 420R in various processor configurations. The web server on both platforms was Apache (v1.3.12). The SSL module on the the Sun Enterprise 420R Server was mod\_SSL (v2.6.6). The SSL module on the The Intel Itanium<sup>™</sup> – based server was RSA's SSL-C.

The Intel Itanium<sup>™</sup> – based server operating system was Turbolinux IA64. The Sun<sup>®</sup> Enterprise 420R<sup>™</sup> server operating system was Solaris<sup>™</sup> 7.

Coradiant used a combination of OpenSSL and proprietary software to measure SSL transaction rates and latency.

In SSL transaction processing, the Itanium<sup>™</sup> processor based server performed more than twelve times the number of SSL connections/sec than the Sun UltraSPARC-II processor.

---

<sup>1</sup> Zona Research claims this threshold is 8 seconds; Gartner and Forrester have listed from 4 to 20 seconds depending on application type and faith that the page contains the sought after content.

## Table of Contents

<i>Abstract</i> .....	2
<i>Table of Contents</i> .....	3
<i>Figures and Tables</i> .....	4
<i>Introduction and Objectives</i> .....	5
<i>Server Configurations</i> .....	5
Server Hardware Configurations .....	5
Server Software Configuration .....	6
Client Configuration .....	6
Network Configuration.....	7
<i>Methodology</i> .....	7
Pre-test .....	7
SSL tests .....	7
<i>Results</i> .....	8
SSL Performance .....	8
Latency .....	9
<i>Discussion</i> .....	12
<i>Conclusions</i> .....	12
<i>Appendix A – Test Validations</i> .....	13
Accuracy of Reported Latency.....	13
Server Saturation .....	13
<i>About Coradiant</i> .....	14

**Figures and Tables**

TABLE 1. LIST OF CONFIGURATIONS TESTED ..... 5

FIGURE 1. NETWORK TOPOLOGY OF TEST ENVIRONMENT..... 7

TABLE 2. TYPICAL CLIENT CONFIGURATION USED TO DETERMINE  
MAXIMUM SSL CONNECTION PER SECOND FOR 9 CLIENTS..... 8

FIGURE 2. SSL MAXIMUM CONNECTIONS/SEC..... 9

FIGURE 3. ITANIUM PROCESSOR SSL LATENCY ..... 10

FIGURE 4. ULTRASPARC-II PROCESSOR SSL LATENCY..... 10

FIGURE 5. ONE PROCESSOR COMPARISON, ULTRASPARC-II  
VS ITANIUM PROCESSOR ..... 11

FIGURE 6. FOUR PROCESSOR COMPARISON, ULTRASPARC-II  
VS ITANIUM PROCESSOR ..... 11

TABLE 3. LATENCY REPORTED BY TEST CLIENT VS. LATENCY OBSERVED ON  
THE NETWORK ..... 13

TABLE 4. SERVER PERFORMANCE WITH VARYING CLIENT THREADS ..... 13



## Introduction and Objectives

Coradiant Research benchmarked the SSL transaction performance of the Itanium™ processor. The goals of these tests were as follows:

- Determine how many new SSL transactions the Itanium™ – based server, with various numbers of processors, could perform per second.
- Measure the average latency for an SSL transaction at various loads on the different server configurations.

An important factor in e-commerce systems is not only the number of simultaneous concurrent users that can be served by the system, but also the responsiveness with which these users are served.

- Determine the impact of SSL transactions on a different processor architecture by performing the above tests on a Sun Enterprise™ 420R server.

## Server Configurations

The two server platforms used in this series of testing were: Intel Itanium – based server and the Sun Enterprise 420R (UltraSPARC-II).

The series of tests performed in the Coradiant Research laboratory were on the server platforms described below.

### Server Hardware Configurations

The server hardware platforms used for the tests were the following:

- **Itanium - based server:** 800MHz C0<sup>2</sup> processor, 2 GB of RAM with 4 MB of level 2 cache.
- **UltraSPARC-II - based server:** 450 MHz, 4 GB of RAM and 4 MB of level 2 cache.

Processor	Freq. (MHz)	L2 Cache	FSB (MHz)	# CPUs	RAM GB	Server	cxn
Itanium C0*	800	4M	133	1	2	Itanium based	SSL
Itanium C0*	800	4M	133	2	2	Itanium based	SSL
Itanium C0*	800	4M	133	4	2	Itanium based	SSL
UltraSPARC-II	450	4M	100	1	4	E420R	SSL
UltraSPARC-II	450	4M	100	4	4	E420R	SSL

\*C0 is a near production level stepping of the processor

Table 1. List of configurations tested

<sup>2</sup> C0 is a near production level stepping of the Itanium processor.

## Server Software Configuration

The operating system on the Itanium – based server platform was Turbolinux IA64 with kernel version 2.4.2. The operating system on the Sun Enterprise 420R was Solaris 7, tuned with the following parameters:

- The maximum allowable file descriptors per process was increased to 4096.
- The TCP queue depth was increased to 2048.
- The TCP hash table size was increased to 4096.
- The TCP Time\_Wait period was decreased to 30 seconds.

The tuned parameters on the Sun Solaris OS allowed the system to handle more load generated by the client computers.

The web server in both the UltraSPARC-II and Itanium - based servers was Apache version 1.3.12. Apache server code was compiled individually on each of the UltraSPARC-II and Itanium - based server architectures. No changes were made to the Apache code.

The SSL module used on the Sun UltraSPARC-II - based server was mod\_SSL v2.6.6. The SSL module on the Itanium - based server used was RSA's SSL-C module, which is incorporated into the publicly available binaries to take advantage of the Intel Itanium architecture.

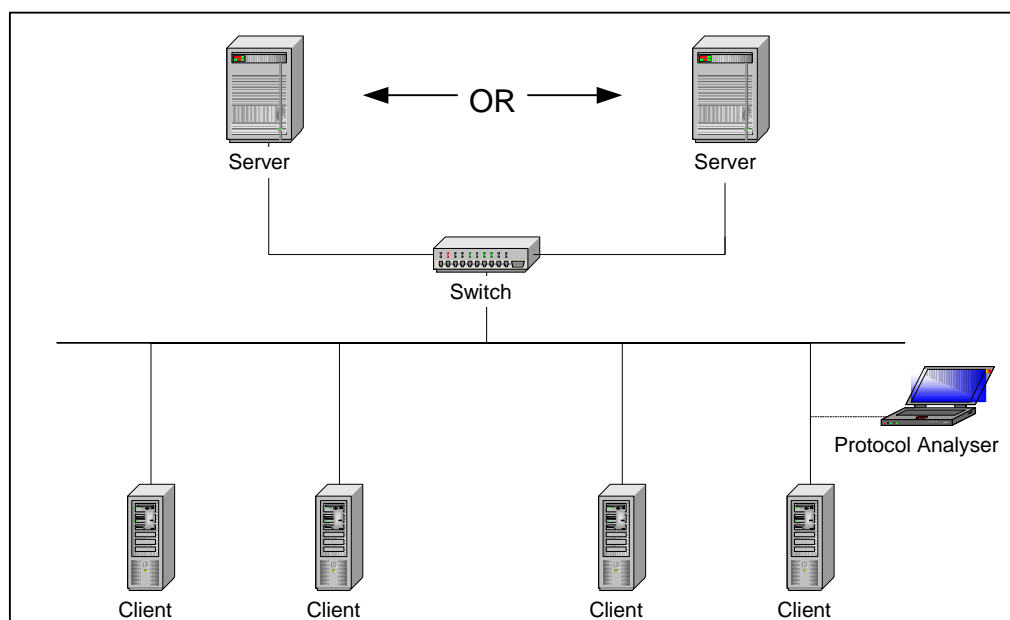
The Apache server on both servers was configured with no logging and the maximum number of servers was set to 256. In addition to this, the "httpd" children were configured to process an unlimited number of requests to avoid forking during the tests. HTTP 1.1 keepalive feature was disabled, as was SSL session key re-use.

## Client Configuration

- Seven to nineteen client computers were used to generate the load for the SSL performance tests. The client computers (client/s) were Intel Pentium™ III 800 or 833 MHz systems with 256 Mbytes of RAM and 256K of level 2 Cache.
- The clients' operating system was the Linux RedHat 6.2 distribution.
- The SSL latency tests were done using a proprietary software client originally developed by Networkshop.
- The SSL maximum new connections/second tests were obtained using OpenSSL client software version 0.9.5.
- All tests performed requested a 2048-byte static html file from the server.
- All SSL tests used **SSL Version 3, RSA authentication (1024 bit key)** using **RC4** stream cipher (128 bit key) and **MD5 HMAC**. In all the SSL tests, SSL session key re-use was disabled and one request for the 2048 byte file was made for each new connection.

## Network Configuration

Each client used a single Intel Ether pro 100 Ethernet network interface card. All clients were connected to a 100 Mbit switch and the network interfaces were all set to 100baseT, full duplex.



*Figure 1. Network topology of test environment*

## Methodology

### Pre-test

Pre-tests were needed to determine the number of threads per client and the number of clients to be used for the testing phase.

The number of threads per client was optimized to achieve the maximum number of connections per second. In each configuration, the SSL client optimum number of threads/client vs. the maximum new connections per second were found by trial and error for each SSL test using OpenSSL. Starting at 60 threads/client with increments of 5-10 threads/client for each test was used to determine the optimal number to generate the maximum new connections/second for each server platform and processor configuration combination.

### SSL tests

The maximum number of new connections per second was found for each server configuration as well as latency measurements at the maximum number of connections/second and at several points below the maximum number for graphing the results.

### Maximum connections/second

The maximum number of new SSL connections/second was determined by the following:

- Depending on the test configuration, 7-19 clients would continuously generate requests over a period of 3 minutes. Each test reported the maximum number of new connections/second.
- The test above was run 3 times and the average of the 3 test runs was used as the maximum number of new connections/second.

Client Parameters	
Threads/client	125
Threads total	1125
Trial duration(s)	180
File size (bytes)	2048

*Table 2. Typical client configuration used to determine maximum SSL connection per second for 9 clients*

### Latency

Latency measurements were done at the maximum new connections/second and at four other points below the maximum determined by the following formula:

**Integer value of  $\{(\text{maximum connections/second}) / 5 \times (\text{point number})\}$ .**

The graph point number ranged from 1 to 4; in total 5 points were used in the latency graphs, the fifth graph point being the maximum number of connections per second graphed against the latency found at that rate of connections/sec. The clients were configured to run the Networkshop SSL client, which was throttled to run at each point the associated number of connections/sec, determined from the formula above. Three test runs for each value of new connections/seconds were done. The average latency measured of the three test runs was used as the final value for latency at the specified graph point.

Seven to nineteen clients were used in the latency tests depending on the combination of number of connections/sec and number of clients need to generate the throttled number of SSL connections. In all the tests involving the Itanium – based server, 19 clients were used for the exception of a single Itanium processor in which 15-19 clients were used. Seven clients were used only on the Sun Enterprise 420R in single processor configuration.

## Results

### SSL Performance

SSL transactions appear to be limited directly by the amount of processor power available to the server. The cryptographic functions of SSL authentication are *sufficiently* demanding that they outweigh I/O functions, or any other bottleneck on the system. This is demonstrated by the linearity with which SSL scales across multiple processors.



The number of new SSL connections that a system can process in one second is linear as we increase the number of processors in a system as seen in Figure 2 below. From the results of this test, the Itanium – based server was able to process more than twelve times the number of new SSL connections/sec than the Sun UltraSPARC-II – based server was capable of handling in comparable processor configuration.

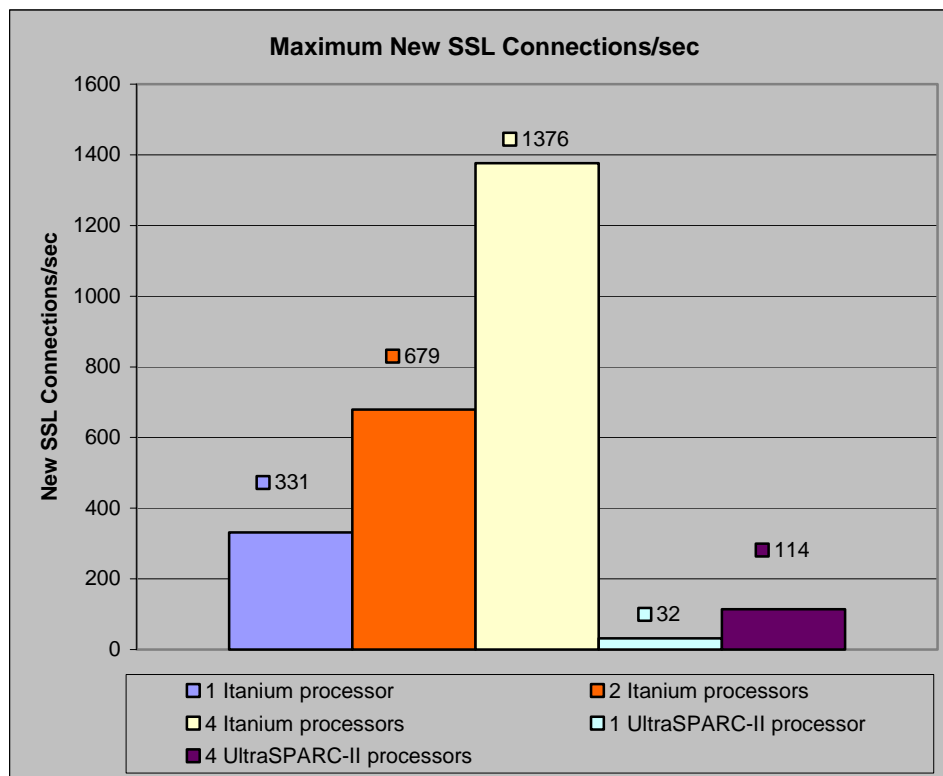


Figure 2. SSL Maximum connections/sec

## Latency

The latency for the various processor configurations is shown in Figure 3 for the Itanium - based server and Figure 4 the UltraSPARC-II - based server.

Lower values of new SSL connections/sec in both UltraSPARC-II and Itanium – based servers exhibited lower latency for lower number of new connections/sec. As the number of connections/sec increased to the maximum capable number of new connections/sec for each system, an exponential increase in latency occurred. The sharp increase in latency at the maximum number of new connections/sec is due to the number of processes backed up waiting in queue. However, the Itanium processor exhibited a more favorable latency by a factor of approximately six over the Sun UltraSPARC-II processor at the maximum number of new SSL connections/sec.

At maximum connections per second, from the graph (Figure 4), the slope for latency on the UltraSPARC-II is greater than that of the Itanium – based server between maximum connections per second and the previous point on the graph.

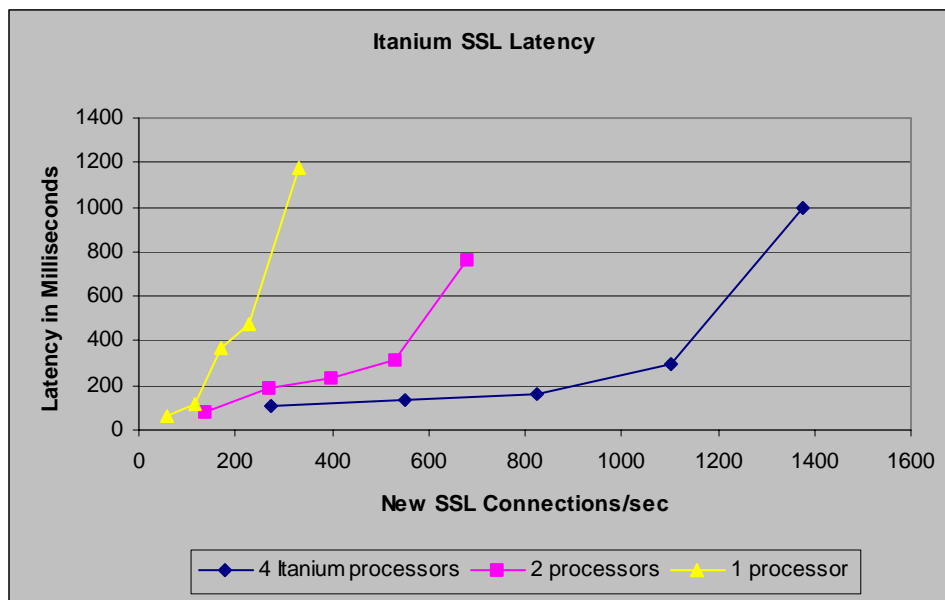


Figure 3. Itanium processor SSL Latency

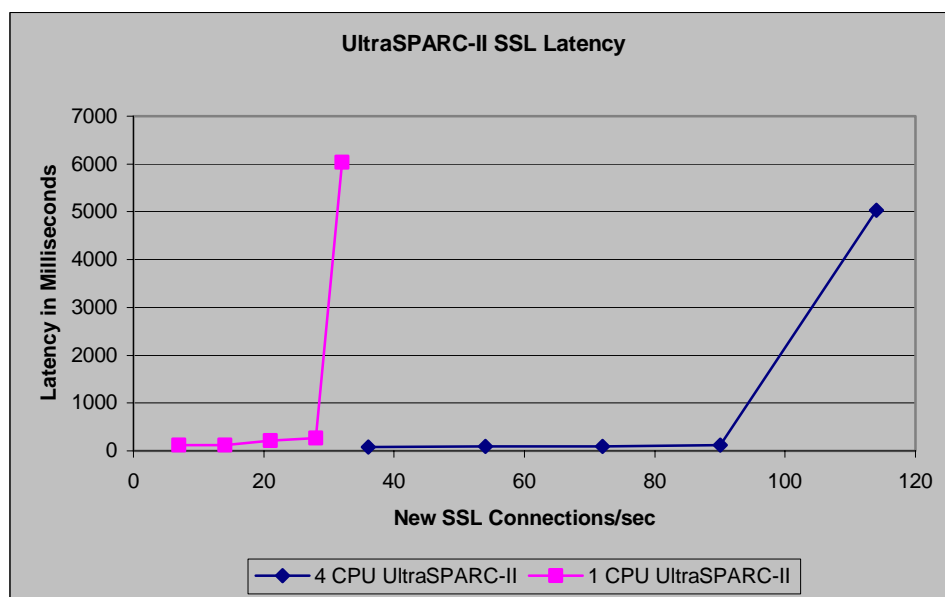


Figure 4. UltraSPARC-II processor SSL Latency

Figures 5 and 6 below superimpose equivalent processor configuration results between the Intel Itanium architecture versus Sun UltraSPARC-II architecture. The Itanium processor response time was 6 times faster at the maximum number of connections/second. The number of maximum connections/second for the Itanium processor was over twelve times greater than UltraSPARC-II processor. In each of the superimposed graphs Figures 5 and 6, each equivalent processor configuration of the UltraSPARC-II vs. Itanium processor, the SUN UltraSPARC-II – based server bottlenecked at less than twelve times the number of connections per second compared to the Itanium – based server.

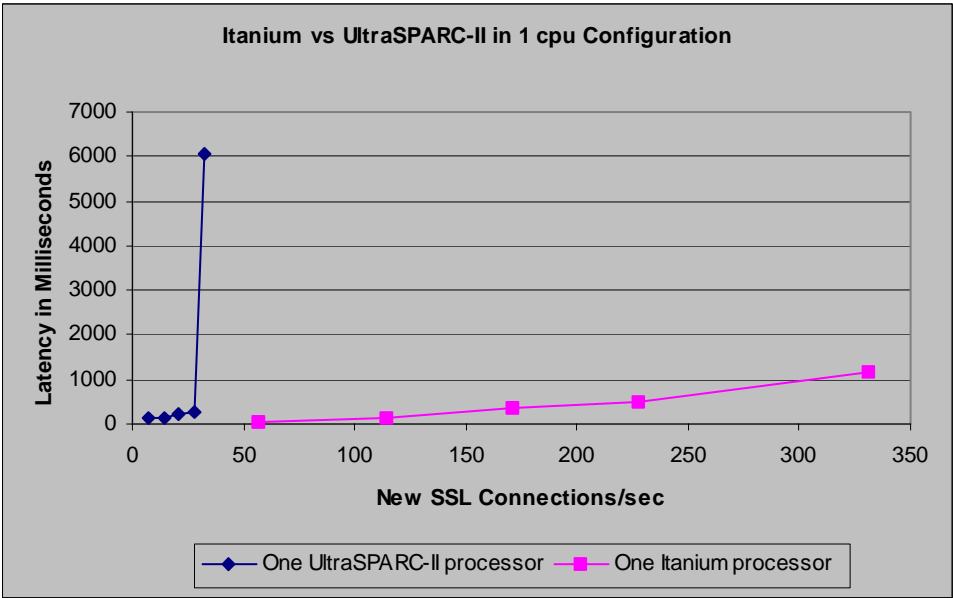


Figure 5. One processor comparison, UltraSPARC-II vs Itanium processor

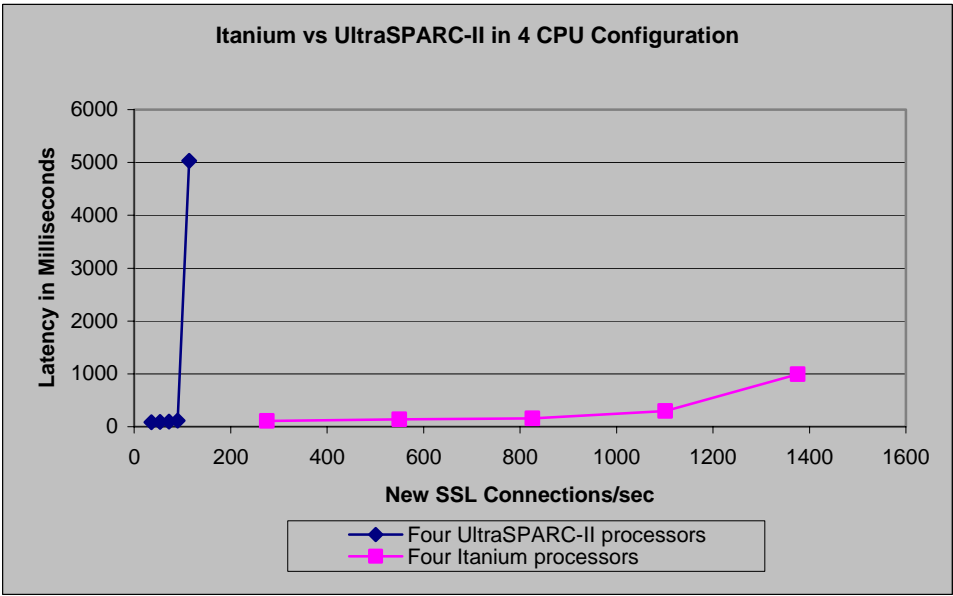


Figure 6. Four processor comparison, UltraSPARC-II vs Itanium processor

## Discussion

Critical issues for today's e-business are Web server SSL connection capacity and latency. As a data transport medium, the Internet can be unreliable. Network conditions, such as overburdened networks, telecommunication company peering points with packet loss, etc, play a major factor in the end-user's perceived experience and satisfaction. Network related problems coupled with overburdened servers (servers that cannot process connections and requests within the end-user "patience time limit<sup>3</sup>"), further amplify this challenge and will result in e-business loss for corporations. As more organizations turn to SSL processing, even for non-confidential data, processing connections and delivering content quickly, will play a major factor in organizations' Internet e-business presence.

A server must handle and scale to the number of connection requests to serve up content to an end-user within a short time period. During peak periods connection time/rate and latency play a crucial role in the end-user experience.

When servers are overburdened with SSL processing, there are other methods to prevent systems from bottlenecking to increase the scalability of SSL processing such as:

- Load Balancing
- Session key re-use, this would relieve the processor of the heavy mathematical computation in key generation
- Using HTTP 1.1 connections so multiple objects may be retrieved in one connection.

These are just some of the methods that can be implemented to relieve overburdened network servers.

## Conclusions

At 1.78 times the clock speed of the UltraSPARC-II processor, the Itanium processor was capable of handling over 12 times the number of SSL connections per second. The number of SSL connections per second as seen from Figure 2 is scalable by a factor of the number of processors in a server. Therefore, scaling the number of processors in a server will increase the number of connections the system can handle linearly. However, this may be limited eventually by other factors such as contention for other system resources.

Latency figures for both server systems at lower numbers of connections per second were quite favorable in SSL connection processing and well under the average end-user expected response time. In the results from latency tests, the UltraSPARC-II – based server began to bottleneck at lower number of connections per second compared to the Itanium – based server. In practice, a server is never run at the maximum number of connections per second, however, the Itanium processor demonstrated (from Figures 5 and 6) it can scale further to keep latency to a minimum where the UltraSPARC-II processor began to bottleneck earlier on when number of SSL connections per second became excessive.

---

<sup>3</sup> Zona Research claims this threshold is 8 seconds; Gartner and Forrester have listed from 4 to 20 seconds depending on application type and faith that the page contains the sought after content.

## Appendix A – Test Validations

### Accuracy of Reported Latency

A packet analyzer validated the custom software used for latency measurements. A packet header trace of TCP SYN and FIN packets was captured and analyzed. The total time of each SSL transaction was recorded both by the header trace and from the test client. The observed latency with the protocol analyzer differed by no greater than 2.3%. These tests were performed in February 2000.

Requested Cxn/Sec	Client reported latency (ms)	Observed Latency (ms)	% difference
50	42	43	2,3
100	60	61	1,6
150	100	101	1,0
200	222	225	1,3

*Table 3. Latency reported by test client vs. latency observed on the network*

### Server Saturation

In order to show that 1995 threads completely saturated the server, we tested the maximum number of connections per second at 1140, 1710, 1995 and 2280 threads. 1995 threads obtained the best results.

Threads	Cxn/sec
1710	327
1995	331
2280	324

*Table 4. Server performance with varying client threads*

## About Coradiant

Coradiant Inc. is a Managed Service Provider (MSP) that provides complete outsourcing of Internet infrastructure services for complex sites and online applications. The company's OutSmart services keep business-critical sites running securely and responsively. Sites are remotely managed, maintained, and proactively monitored from Coradiant's network operations centers. All of Coradiant's customers get access to leading network experts that can help bring new sites online quickly while avoiding expensive equipment purchases. Corporate headquarters are in Boston, MA, with regional offices in California, New Jersey, and New York. The company's international operations are based in Montreal. For more information call 1-877-731-PASS (7277) in North America.

### For more information

Coradiant offers comprehensive services from top-tier data centers across North America. For more details, contact one of our account representatives about the best location and the range of services that will put you online reliably, quickly, and affordably.

**1-877-731-PASS (7277)**  
**WWW.CORADIANT.COM**

© 2001 Coradiant Incorporated. All rights reserved.

The information in this report is proprietary and confidential. This report may not be copied in whole or part without prior written consent from Coradiant Research.

#### Trademarks

Itanium™ is a registered trademark of Intel Corporation or its subsidiaries in the United States and other countries. Solaris™ and UltraSPARC™ are registered trademarks of Sun Microsystems or its subsidiaries in the United States and other countries. All other company and product names may be trademarks of their respective owners.